OVERSIGHT

TABLE OF CONTENTS

Abbreviations Used in This Report

ANL-W	Argonne National Laboratory-West
CH	DOE Chicago Operations Office
DOE	U.S. Department of Energy
ID	DOE Idaho Operations Office
INEEL	Idaho National Engineering and Environmental Laboratory
PSAP	Personnel Security Assurance Program
SRT	Special Response Team

1.0 Introduction

The Office of Security Evaluations conducted this review to determine the status of issues identified in April 1996.

The mission of the Office of Oversight embraces not only the evaluation of safety and safeguards and security management performance, but also a commitment to ensuring that the issues or concerns identified during its evaluations are brought to a satisfactory resolution in a timely manner. To support this commitment, the Office of Oversight conducts followup reviews of safety or safeguards and security management concerns.

In April 1996, the Office of Oversight, through its subordinate Office of Security Evaluations, conducted an evaluation of safeguards and security management performance at the Argonne National Laboratory-West (ANL-W). This evaluation highlighted several management concerns. Detailed background with respect to these concerns is contained in the April 1996 Office of Security Evaluations report on the evaluation of ANL-W, which was classified Secret/NSI. In May 1996, these concerns were transmitted to the Office of Oversight's Office of EH Residents, whose mission includes monitoring progress toward the resolution of such concerns. The Office of Security Evaluations and the Office of EH Residents scheduled a formal followup review, which was completed on November 20, 1996. The results of this followup review are the subject of this report.

2.0 Results

The followup review focused on seven areas.

Seven specific management concerns were identified by the Office of Security Evaluations as focus areas for the followup review:

1. **An operational feature associated with several special security doors**
2. **Potential climbing aids located in close proximity to security clear zone fences**
3. **Inclusion of all required personnel in the Personnel Security Assurance Program (PSAP)**
4. **Reliance upon single, non-complementary alarm sensor systems to protect certain significant security assets**
5. **Impact of changes in the protective force response posture at the Idaho National Engineering and Environmental Laboratory upon tactical response at ANL-W**
6. **Full implementation of computer security requirements**
7. **Full compliance of material control and accountability performance testing procedures with DOE requirements and good program practices**

The current status of these concerns, as determined by the followup review, is discussed below.

Special Security Doors

A concern was noted during the evaluation with respect to the operation of several security doors (specific details of this concern are classified).

Concerns related to the adequacy of special security doors have been resolved.

ANL-W undertook several measures to resolve this concern. The most fundamental measure involved removing the security asset in question from the location protected by these doors; this action, completed on October 31, 1996, negated the concern associated with these doors. In response to secondary concerns, ANL-W reconfigured the electrical power supply to these doors. The Office of Security Evaluations regards this concern as resolved.

Potential Climbing Aids

Protective force personnel have received instruction on how an adversary could use climbing aids to bypass intrusion detection systems.

During the evaluation, the presence of several potential climbing aids, which could be used to scale fences and circumvent alarm sensors, was noted in security clear zones. Analysis of the underlying causes of this situation indicated that although protective force personnel understood the need to check fence lines to determine that no climbing aids had been placed nearby, they did not understand the function of the various intrusion detection systems in place at these locations. Since they did not understand how these systems functioned, they could not appreciate the way in which climbing aids could be used to bypass the alarm sensors. ANL-W has since provided instruction to protective force personnel with respect to the general capabilities of the intrusion detection systems.[1] Since protective force

[1] This training included viewing the "Physical Security Systems: Lessons Learned" videotape produced by the Office of Security Evaluations and an orientation session conducted by a member of the Office of Security Evaluations Composite Adversary Team who now serves on the security staff at ANL-W.

personnel now have a better understanding of how a potential adversary might attempt to exploit the presence of climbing aids, they are better prepared to recognize potential problems and intervene appropriately. This concern is regarded as closed.

Inclusion of Appropriate Personnel in the PSAP

Some progress has been made in including all appropriate personnel in the Personnel Security Assurance Program.

The management evaluation determined that not all personnel at ANL-W who meet the Department of Energy (DOE) order criteria for inclusion in the PSAP program had in fact been included, as required by Federal regulation (10 CFR Part 710). In response to this determination, ANL-W and DOE Chicago Operations Office (CH) management made a commitment to review this issue and, where indicated, to increase the numbers and categories of personnel to be included in the PSAP. This study resulted in the number of PSAP-designated personnel increasing from 12 to 78. The ANL-W PSAP Administrator indicated during this followup review that the only task remaining to complete the processing of these additional personnel was the interview process for the Employee Assistance Program. According to the program administrator, approximately 25 percent of these interviews have been completed. The administrator also indicated that once the interviews were completed, the PSAP packages would be submitted for medical review before finally being sent to the PSAP approving official at the DOE Idaho Operations Office (ID).[2]

However, subsequent interviews with the ID PSAP Approving Official indicated that, as of the conclusion of this followup review, ID had received only seven PSAP application packages out of the 66 proposed applicants from ANL-W. Furthermore, the ID representative noted that although these seven packages were accompanied by a cover memorandum, the DOE requirement specified that justification statements be included with each individual package. For this reason, no action had been taken to process the seven applications. This situation was relayed to the ANL-W PSAP Administrator by a member of the followup review team.

Concerns about the random drug testing process have been resolved.

A related issue addressed during this followup review involved the drug testing program associated with the PSAP. The Office of Security Evaluations management evaluation in April noted that the random selection process for drug testing, as implemented by ANL-W, did not achieve the required annual random testing of the entire PSAP population. The process that was implemented resulted in directed testing of some participants prior to annual recertification; this approach defeats the purpose of the random testing requirement. Further investigation during the followup review indicates that the practice now implemented at ANL-W more closely approximates the intent of the PSAP requirements. Specifically, although some personnel are not tested prior to their birth months during some years, they are nonetheless tested randomly within the birth month, and, once tested, are returned to the random pool for testing in the subsequent year. Therefore, no PSAP employee is in a position to predict the date of the actual test.

Although the random drug testing concern may be regarded as closed, the concern associated with the inclusion of appropriate personnel in the PSAP remains open. This concern will continue to be monitored by the Office of Security Evaluations and the Office of EH Residents.

[2] Instead of maintaining a separate PSAP program, ANL-W participates in the larger program maintained by ID.

Complementary Alarm Sensors

There is no systematic process in place for assuring complementary alarm sensors at all appropriate locations, though some positive steps have been taken.

As a result of potential concerns noted during the management evaluation, ANL-W reviewed its practice of relying upon single, non-complementary alarm sensors to protect certain security assets. This led to the decision to install a second complementary sensor system at two locations highlighted during the management evaluation. Installation at one of these locations has now been completed, and a work order has been issued for installation at the second location. Viewing the potential concern as a whole, ANL-W representatives indicated during this review that "some thought" has been given to installing complementary systems at the remaining locations surrounding this security area. However, no supporting documentation for this final step was evident. ANL-W similarly resolved a related concern by providing intrusion detection sensor coverage at some locations identified as potential areas for bypassing sensors at the Property Protection Area.

While the measures described above represent positive steps, the current approach at ANL-W remains oriented toward "patching" specific locations, rather than developing a strategic plan to identify and correct potential problems on a more systematic basis. For this reason, this concern remains unresolved and will continue to be monitored jointly by Security Evaluations and the Office of EH Residents.

Protective Force Response Posture

For many years, ANL-W has relied upon the Idaho National Engineering and Environmental Laboratory (INEEL) to provide support in the form of a special response team (SRT) capability.

The transfer of the special response team capability to ANL-W has been completed, and the team is functioning adequately.

During the management evaluation, it was noted that changes in security requirements at INEEL had resulted in the deletion of the INEEL SRT capability. A corresponding decision was made by ANL-W management to develop its own SRT. At the time of the management evaluation, this process had been initiated but not completed. The screening of potential transfer personnel from INEEL's SRT had just started, training of ANL-W protective force members to the SRT standard had not begun, and the new response posture associated with these changes had not been adequately performance tested.

Concerns remain about the lack of practical direction in the tactical response plan.

The followup review determined that the transition to an ANL-W-based SRT has been completed and that the new team appears to be adequately functioning. In response to the performance testing concern, CH subsequently conducted a series of protective force response tests that directly support the new response posture. This concern is thus regarded as resolved.[3]

The followup review addressed an additional question concerning protective force response. During the management evaluation, a disparity was noted between day-shift and night-shift response procedures at a particular location. Although the day shift was required to take immediate action to retake the facility in question and neutralize any potential adversary present inside, the night shift had been given no similar instructions—despite the fact that there

[3] ANL-W has also taken the opportunity afforded by the change in its relationship with INEEL security to staff the ANL-W secondary alarm station. This measure enhances the ANL-W physical security program and addresses a longstanding Office of Security Evaluations issue.

was no difference in the actual protection requirement between the two shifts. Moreover, the protective force personnel on the night shift did not understand that such a response might be needed.

The followup review noted that the recapture requirement on both shifts is now mentioned in the August 1996 revision of the ANL-W tactical response plan. However, the followup review team pointed out to ANL-W and CH representatives that the actual direction provided in the tactical response plan is extremely limited. The lack of detailed direction means that in practice, tactical response would continue to rely upon the "corporate" knowledge of current protective force personnel; such knowledge would almost certainly be outdated. In response to this observation, the CH Safeguards and Security Director immediately directed ANL-W to clarify the requirements in the tactical response plan. Based on CH's response, this concern is considered closed, although Security Evaluations and the EH Residents will continue to monitor the direction provided to the protective force.

Implementation of Computer Security Requirements

A variety of concerns relating to the implementation of computer security requirements were noted during the management evaluation. Training and recordkeeping concerns associated with the transition at that time to a new Computer Security System Manager have been resolved. The concern pertaining to Internet connectivity has likewise been adequately addressed.

Progress has been made in many areas of computer security, although misperceptions persist concerning the Department's overall responsibilities toward sensitive data.

Progress has also been made with respect to the performance of sensitivity determinations on unclassified information. The April evaluation noted that ANL-W made a distinction between DOE sensitive and ANL-W proprietary data, and that ANL-W had determined that approximately 80 to 90 percent of the data at the site was proprietary rather than sensitive. Since ANL-W took the position that DOE cannot inspect or oversee ANL-W proprietary data, a large proportion of the data at the site was automatically excluded from DOE inspection or oversight. The followup review determined that sensitivity determinations are, in fact, performed on all ANL-W data and that CH policy provides for the review of all proprietary data except personnel information and some financial systems data regarded as "incidental to the contract." On this basis, these concerns may be regarded as closed.

During the course of this followup review, the CH Director of Information Resource Management Policy, Planning, and Coordination took the position that the Office of Oversight's responsibility is limited to data contained in computer systems that support safeguards and security, not all data on ANL-W systems. This position is incorrect for a number of reasons. First, it ignores a basic concern, which is that DOE has a responsibility to evaluate the protection of other sensitive data, and this responsibility cannot be fulfilled if only safeguards and security-related systems are evaluated. Second, this artificial limitation places the Office of Security Evaluations in the position of having to accept, at face value, the site's determination as to what information meets the definition of classified or sensitive. This represents a fundamental limitation on the purview of Oversight. It should, however, be noted that the position taken by this CH representative has not been formally endorsed by higher CH management.

Finally, progress has also been made in resolving the concern associated with the procedures for the modification and testing of intrusion alarm processing system software. (Details relating to this concern are provided in the April 1996 management evaluation report.) This concern is being addressed through the inclusion of appropriate personnel in the PSAP.

Responsiveness to the Department's goals regarding waste, fraud, and abuse of computer assets remains an open issue.

The general progress represented by these various steps, however, has not been matched in another area, notably the concerns relating to required audits to control waste, fraud, and abuse. The management evaluation noted that DOE orders require random, unannounced annual audits for computer system waste, fraud, and abuse, unless other equivalent protective measures are employed. It further noted that CH had chosen to grant ANL-W relief from this requirement based upon the "equivalent protective measures" provision and also because of cost considerations. The measures cited as "equivalent" consisted of audits directed by department managers (not computer security managers) *after a perceived abuse is identified*. The Office of Security Evaluations took the position that this approach did not represent equivalent protection, since an audit would be conducted only if a case of abuse happened to come to light. It was further noted that the availability of automated audit tools invalidated much of the site's concern about potentially high costs of unannounced annual audits.

The followup review determined that CH does not intend to re-evaluate the original grant of waiver. CH maintains its original position concerning both protection equivalency and cost considerations. Furthermore, CH notes that the relevant order is currently being revised and that the annual audit requirement may be eliminated. This position, however, is clearly unresponsive to the original concern with respect to equivalency of protection, regardless of the precise language of the order revision. In addition, it is unlikely that the revised order will express indifference to waste, fraud, and abuse. As long as these continue to be items of concern to DOE, the practices currently followed at ANL-W will not fulfill the Department's needs. This concern thus remains open; it will be re-evaluated by the Office of Security Evaluations once the new order is issued.

Material Control and Accountability Performance Testing

Communications with the Headquarters Office of Safeguards and security have resolved issues related to material control and accountability performance testing.

The concerns noted during the management evaluation pertained to the number of performance tests and the inventory sample size employed to validate the minimum level of performance. These concerns have been the subject of an exchange of correspondence between the Office of Security Evaluations and the appropriate policy official in the Office of Safeguards and Security at DOE Headquarters. On the basis of this correspondence, these concerns are now regarded as closed.

3.0 Conclusions

This review finds evidence of management effectiveness in responding to many specific concerns.

The April 1996 safeguards and security management evaluation of ANL-W noted a variety of specific protection and management concerns, as well as an overall concern relating to the need for ANL-W management to approach the application of safeguards and security with a greater degree of rigor and consistency. The evidence of this followup review clearly demonstrates the willingness on the part of ANL-W and CH to respond to particular concerns with credible solutions. This was particularly evident in connection with the concern associated with the special security doors, which was viewed as the most urgent and critical concern identified during the management evaluation. The measures taken by ANL-W with respect to this concern and to such other concerns as tactical response performance testing and Internet connectivity reflect well upon ANL-W and CH safeguards and security management.

Oversight will continue in areas where insufficient management follow-through has been evident.

At the same time, however, the limited degree of follow-through on such matters as the application of complementary sensor systems, the timely completion of PSAP program application packages, the direction provided to tactical response personnel, and the implementation of proactive measures to deter computer system waste, fraud, and abuse suggest the continued need for attention to safeguards and security program practices on the part of senior ANL-W and CH managers. These specific areas have been designated by the Office of Security Evaluations as priority areas for ongoing followup.